

FIG. 10

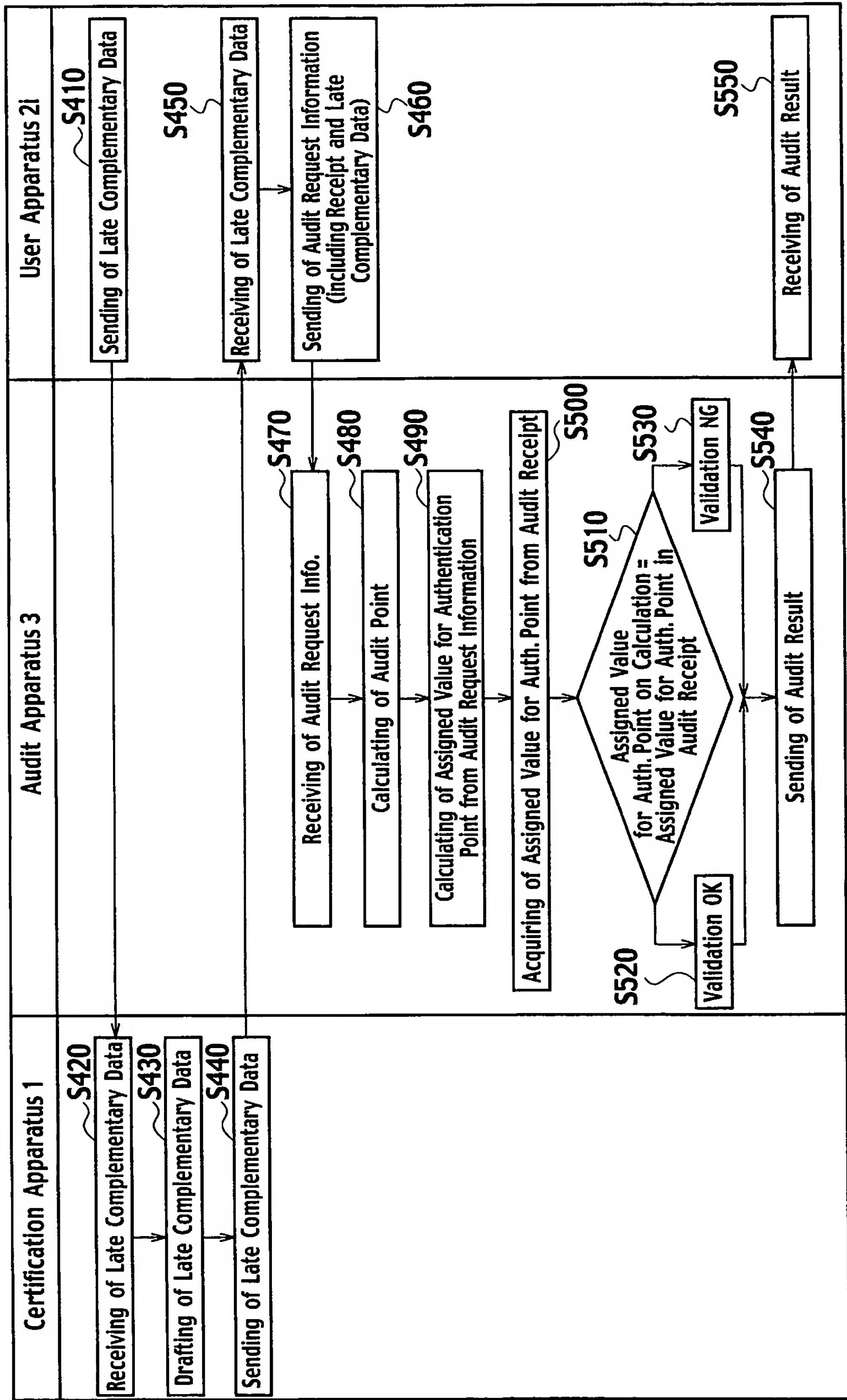


FIG. 15

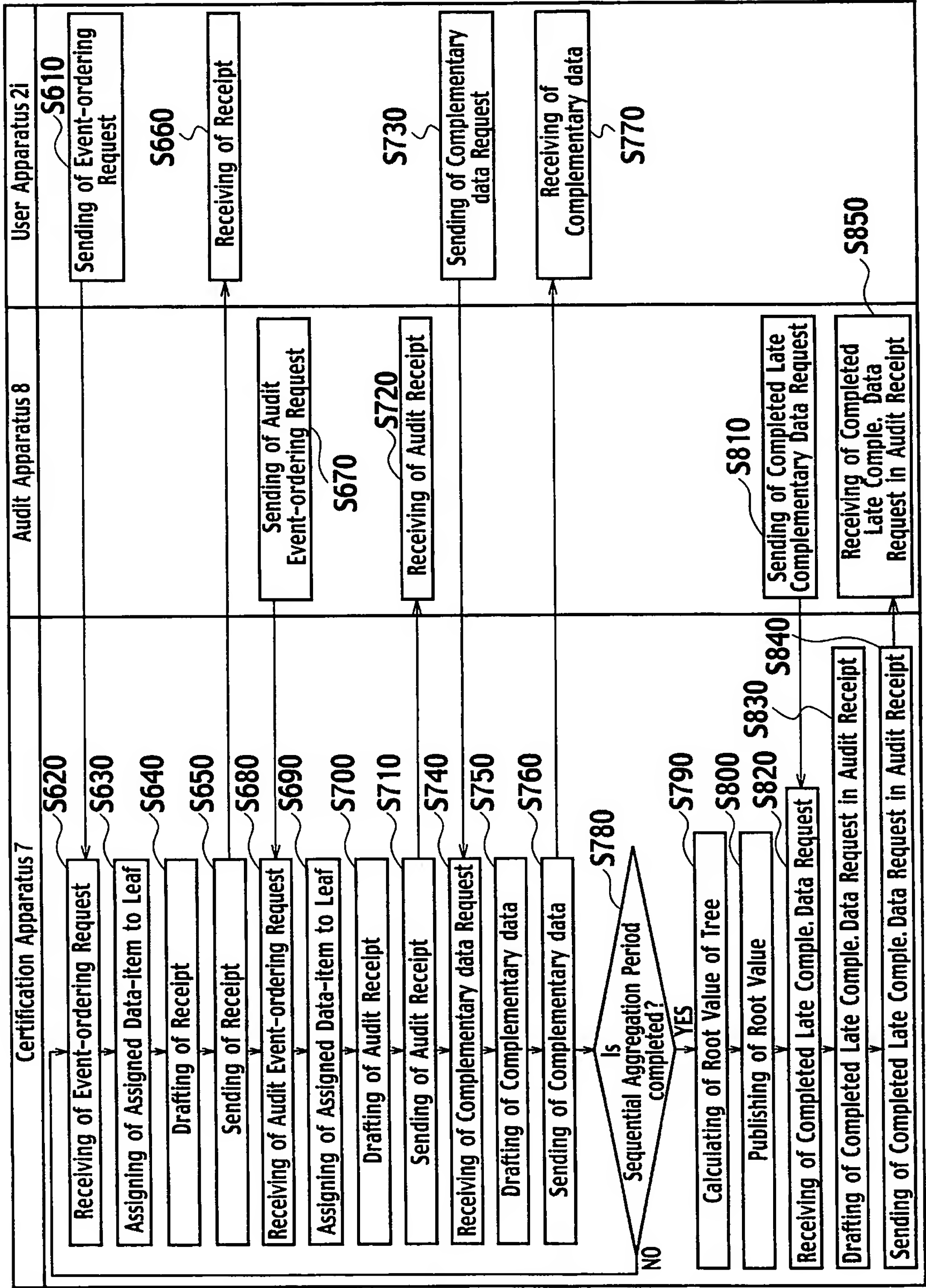
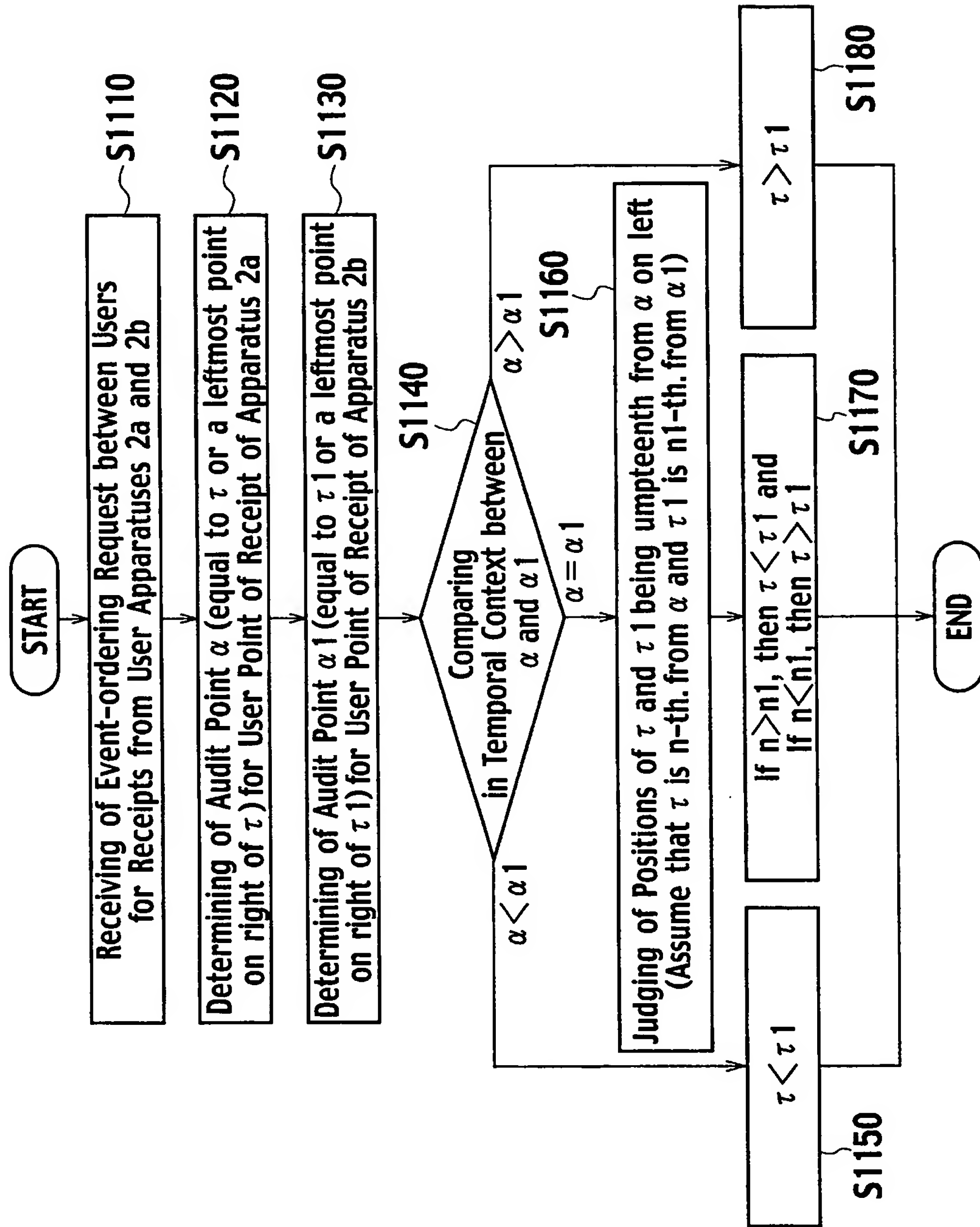


FIG. 17



18 / 77

FIG. 19

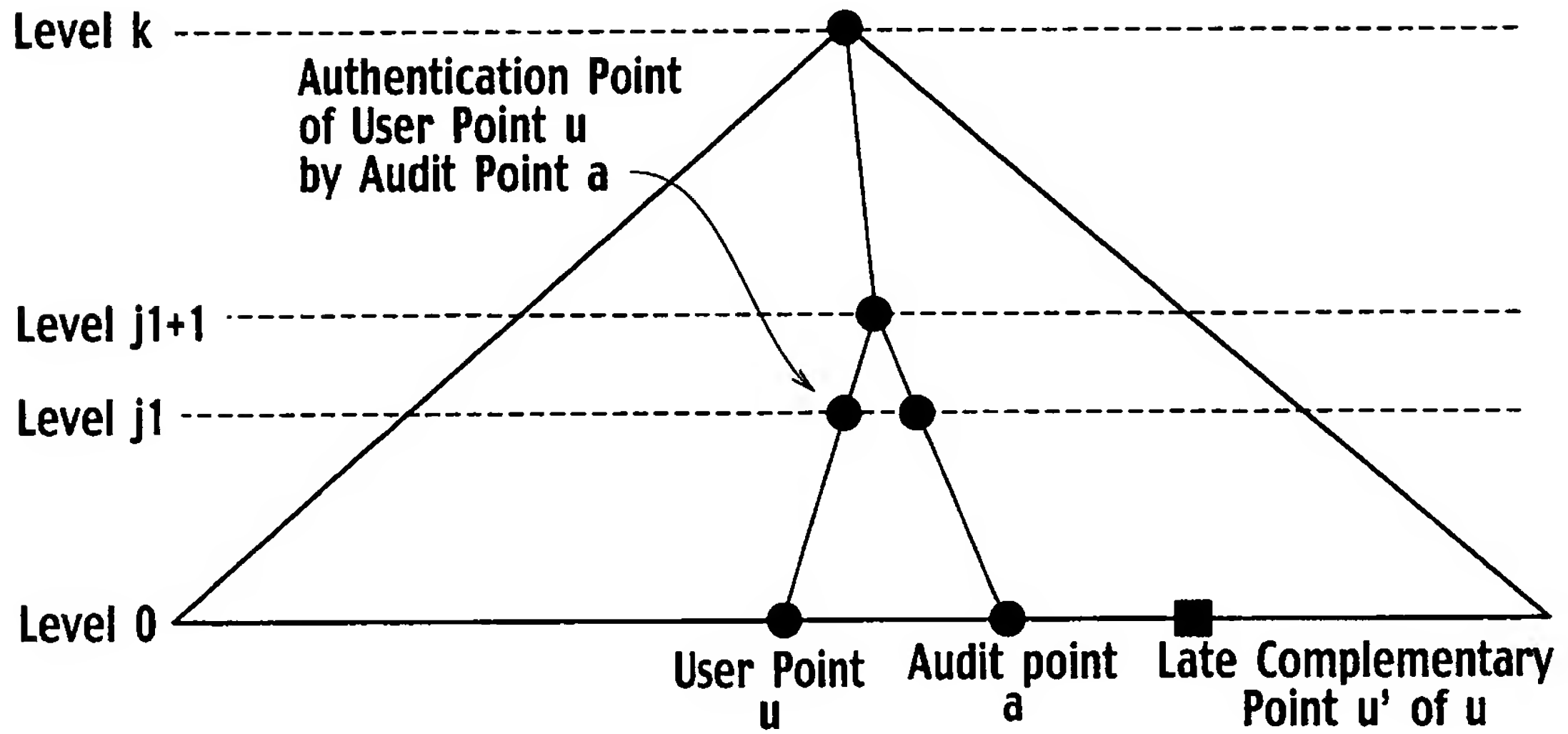


FIG. 20

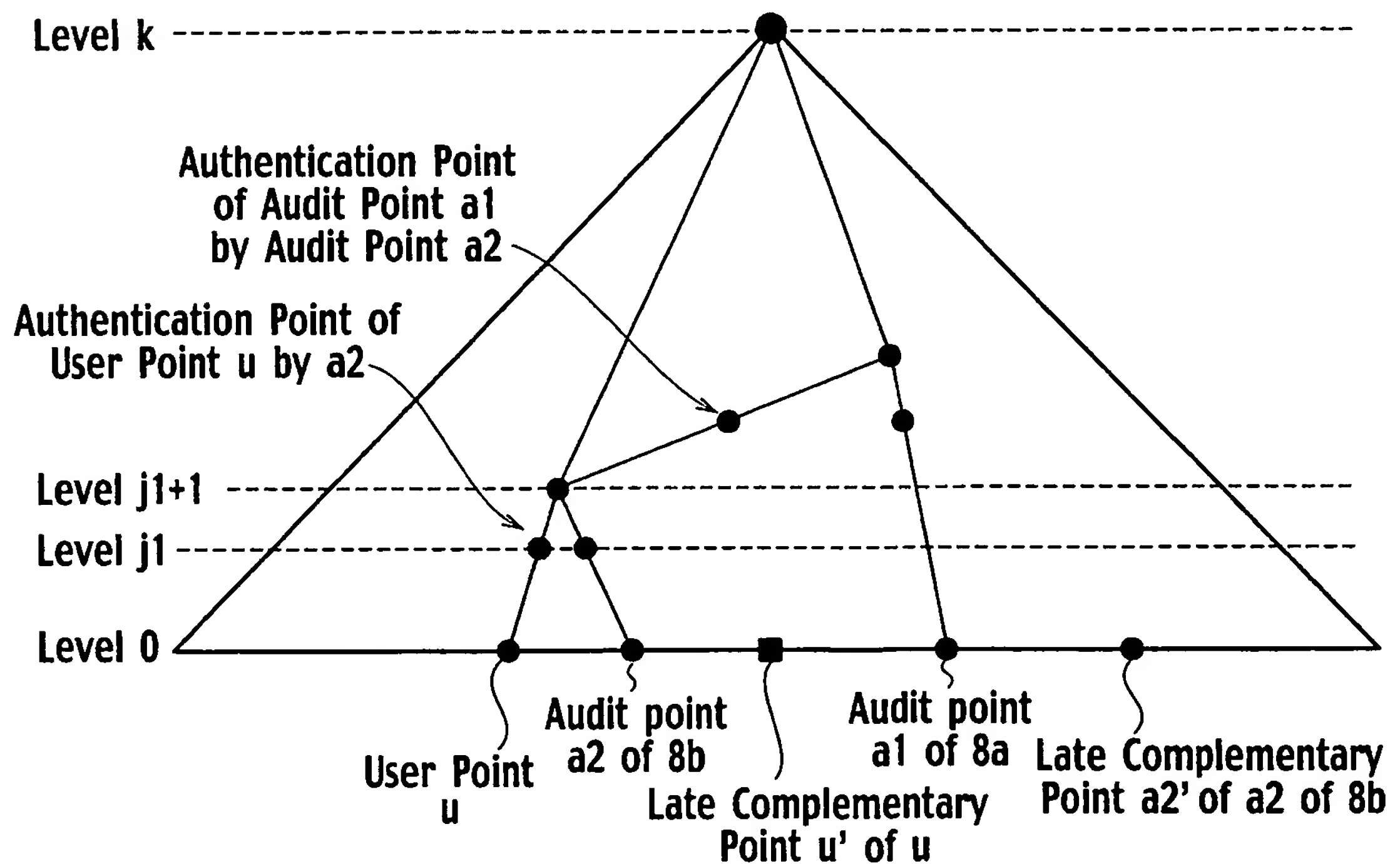


FIG. 24

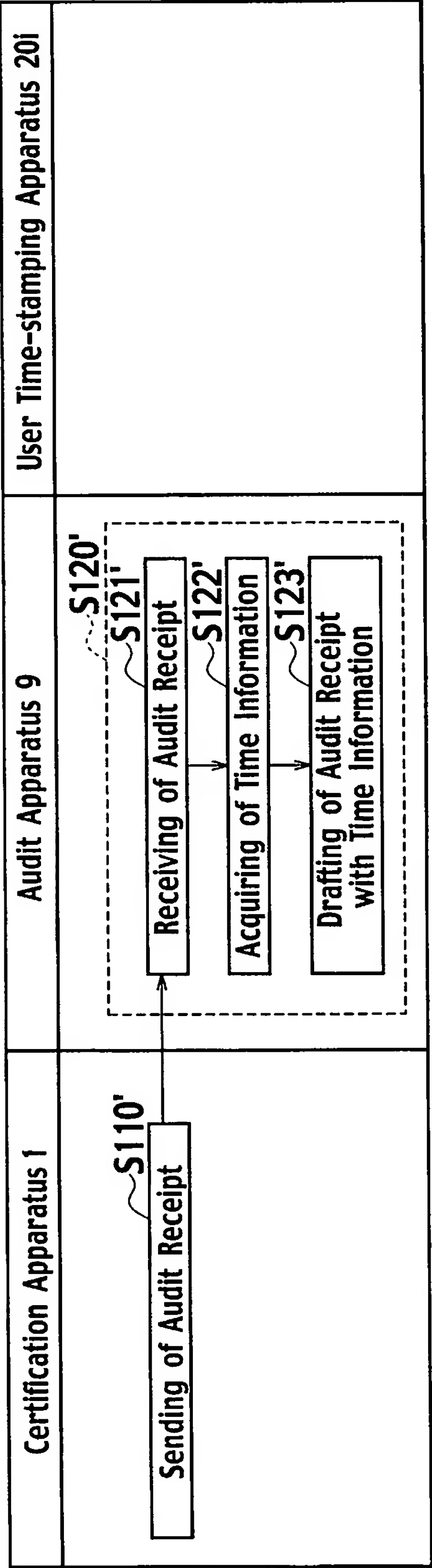


FIG. 25

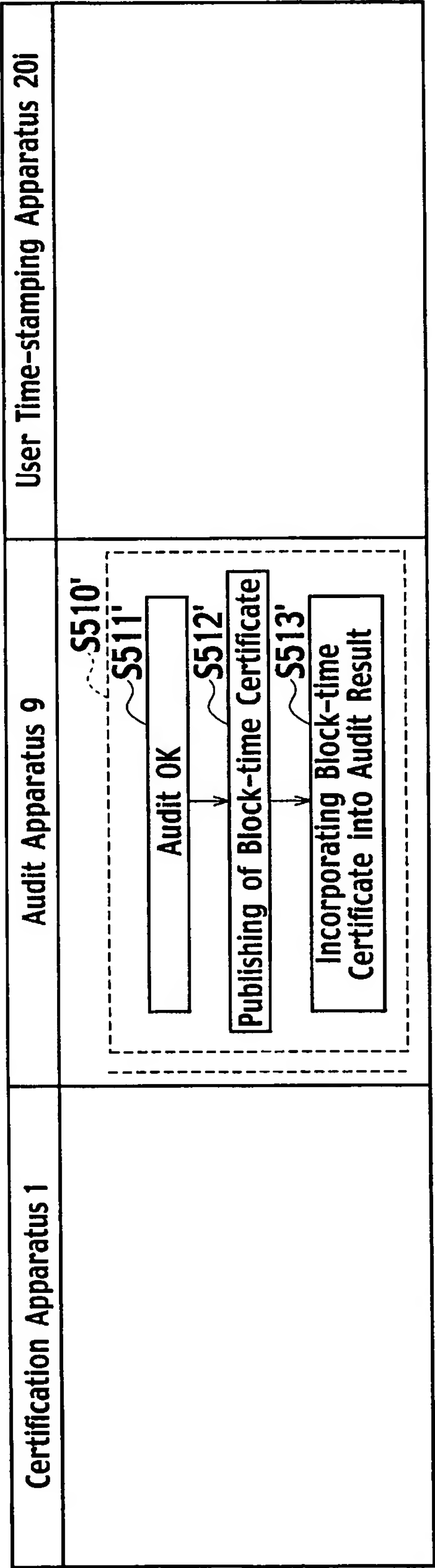
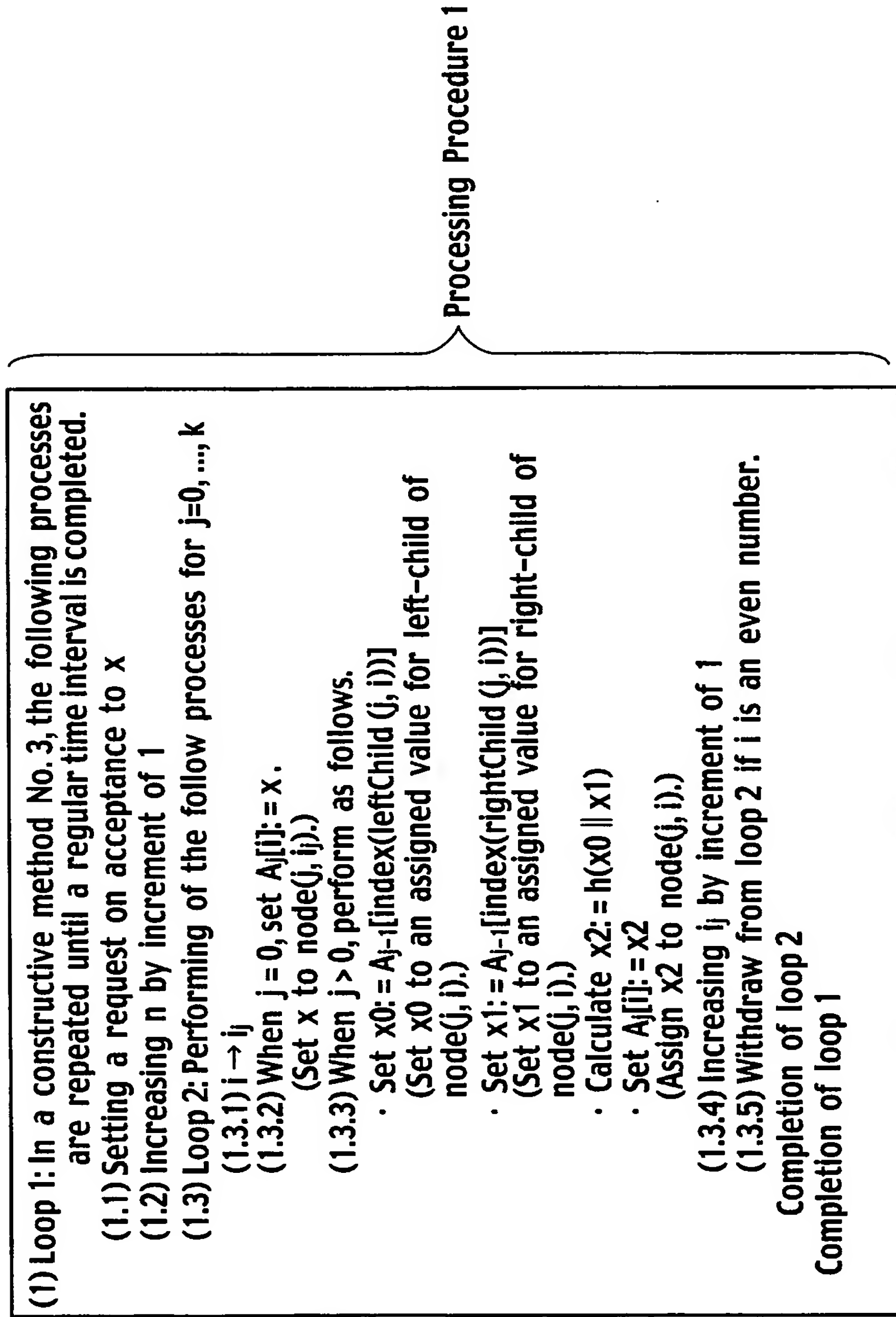


FIG. 27



26 / 77

FIG. 28

- (2) Performing of the following processes after withdrawing from loop 1 on reaching finish time.
- (2.1) Set $k := \text{ceiling}(\log_2(n))$.
 - (2.2) Calculate $\text{rtPath}(k, 0, n-1)$ and Set $((0, r(0), \dots, k, r(k)))$ to the calculation result.
 - (2.3) Loop 3: Performing of the follow processes for $j=0, \dots, k$
 - (2.3.1) $i \rightarrow i_j$
 - (2.3.2) Case of $j = 0$:
 - (2.3.2.1) When i is an odd number:
 - Produce a dummy $r := R(0, i)$
 - Set $A_j[i] := r$
(Assign r to $\text{node}(0, i)$.)
 - Set $b_j := \text{true}$.
 - Increase i_j by increment of 1.
 - (2.3.3) Case of $0 < j \leq k$:
 - (2.3.3.1) When $i = r(j)$:
 - (when $\text{node}(j, i)$ is on $\text{rtPath}(k, 0, n-1)$):
 - (2.3.3.1.1) $x_0 := A_{j-1}[\text{index}(\text{leftChild}(j, i))]$
(Set x_0 to an assigned value for left-child of $\text{node}(j, i)$.)
 - (2.3.3.1.2) $x_1 := A_{j-1}[\text{index}(\text{rightChild}(j, i))]$
(Set x_1 to an assigned value for right-child of $\text{node}(j, i)$.)
 - (2.3.3.1.3) Calculate $x_2 := h(x_0 \parallel x_1)$
 - (2.3.3.1.4) Set $A_j[i] := x_2$
(Assign x_2 to $\text{node}(j, i)$.)
 - (2.3.3.1.5) When i is an even number and $j < k$:
 - Increase i by increment of 1.
 - Calculate $r := R(j, i)$ and Set $A_j[i] := r$
(Assign r to $\text{node}(j, i)$.)
 - Set $b_j := \text{true}$.
 - Set $i_j := i + 1$
 - (2.3.3.2) When $i = r(j) + 1$, an odd number and $j < k$:
 - Calculate $r := R(j, i)$ and Set $A_j[i] := r$
(Assign r to $\text{node}(j, i)$.)
 - Set $b_j := \text{true}$.
 - Increase i_j by increment of 1.
- Completion of loop 3

Processing Procedure 2

FIG. 40

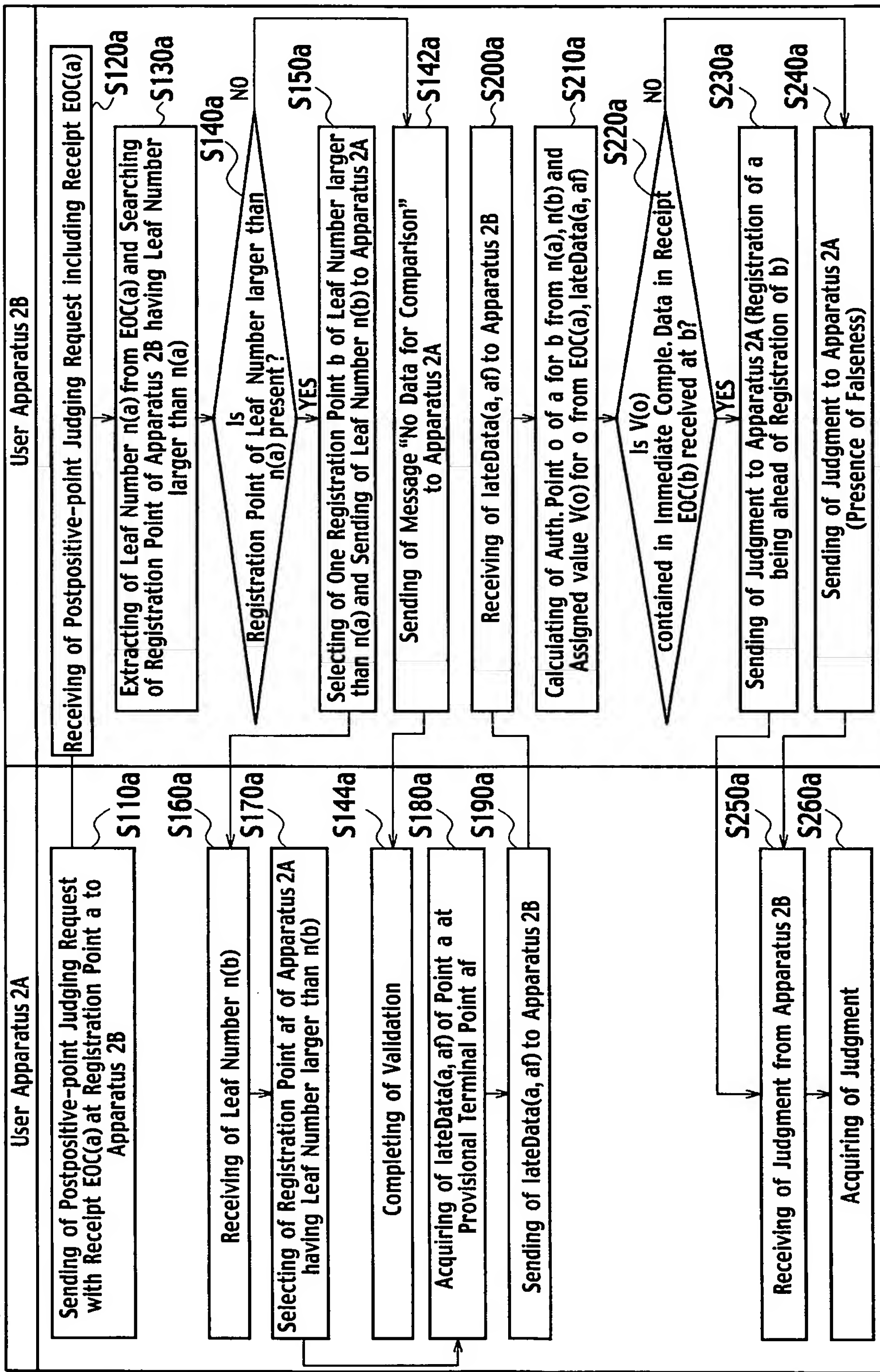
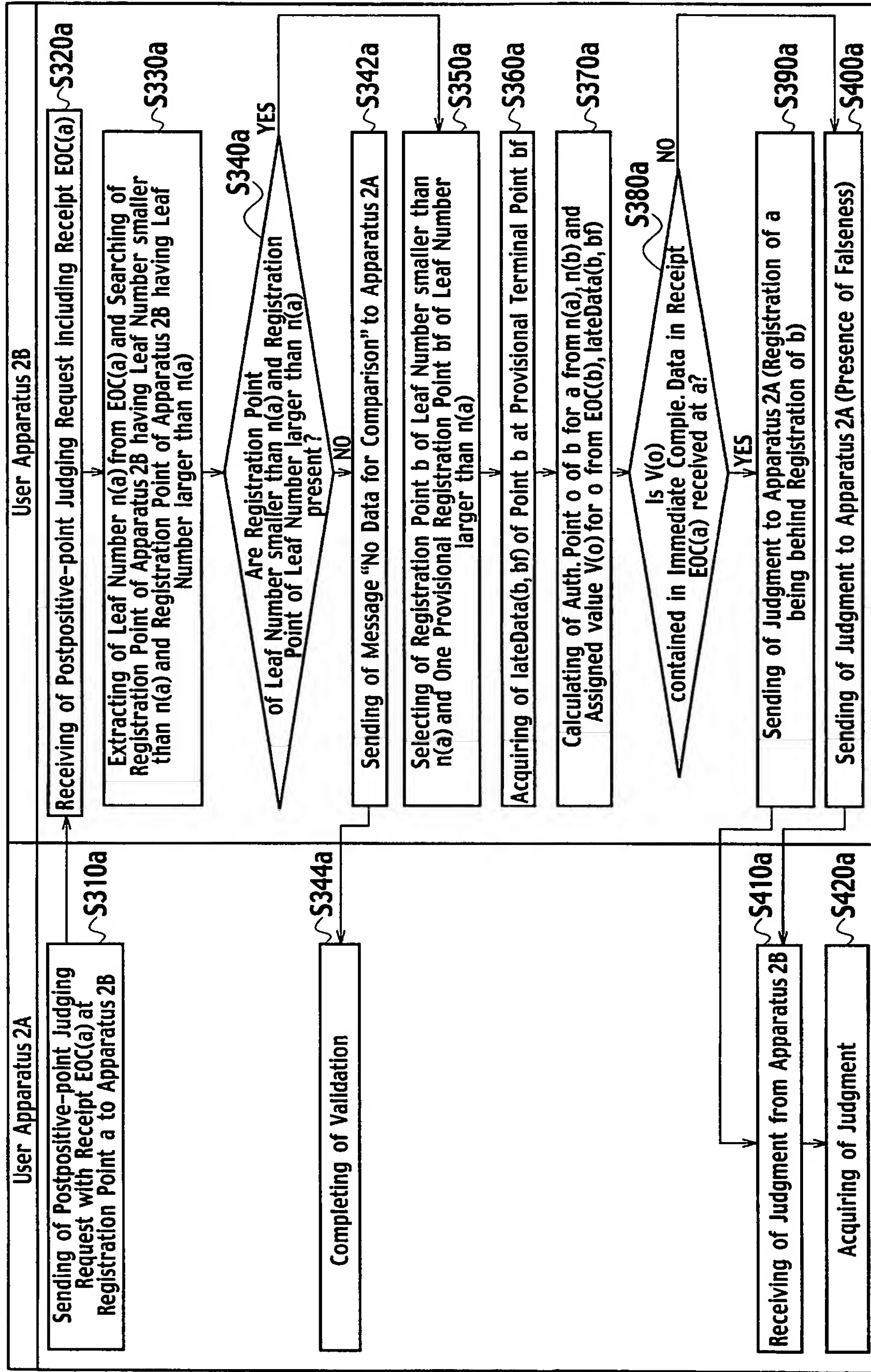
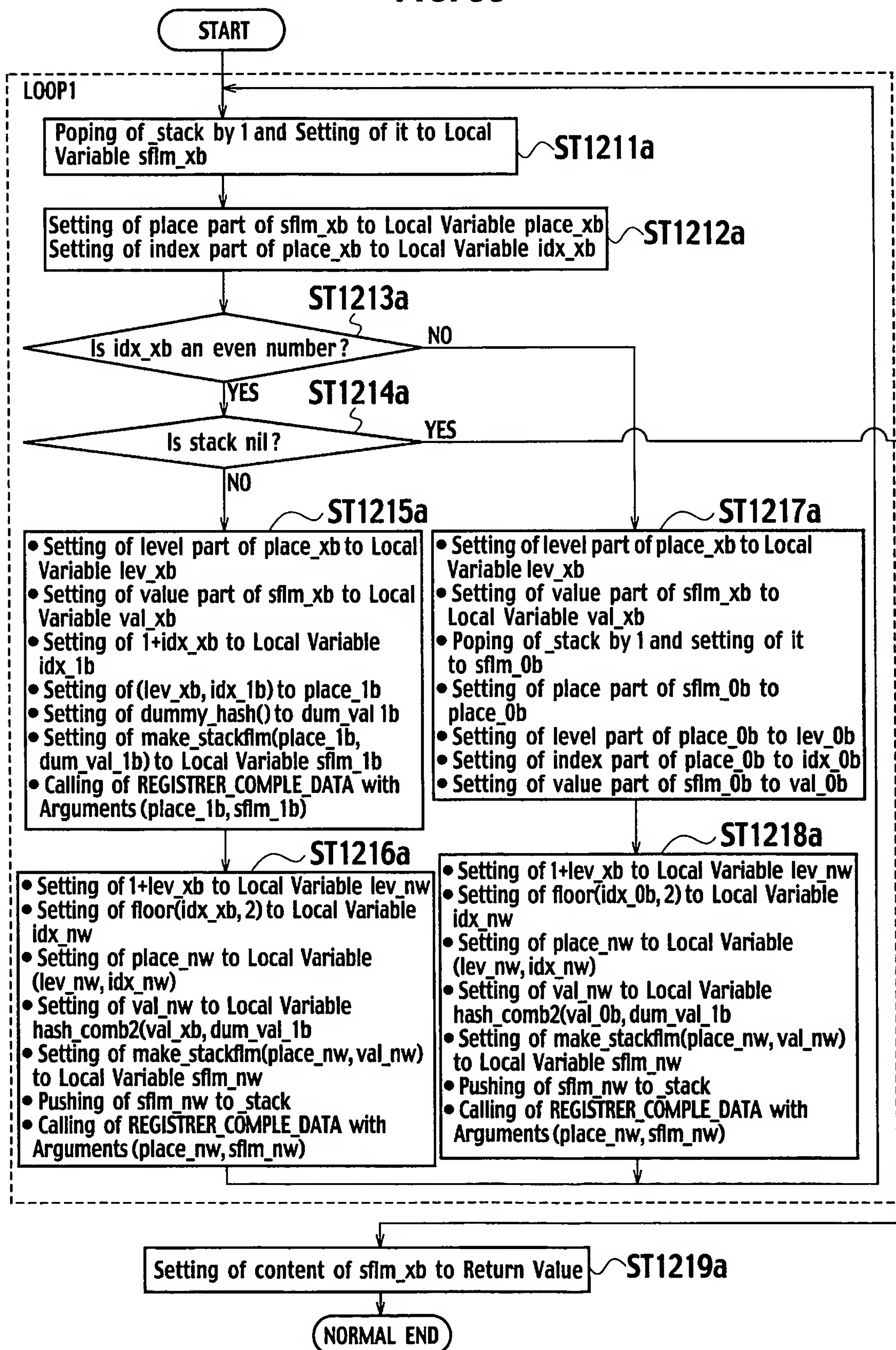


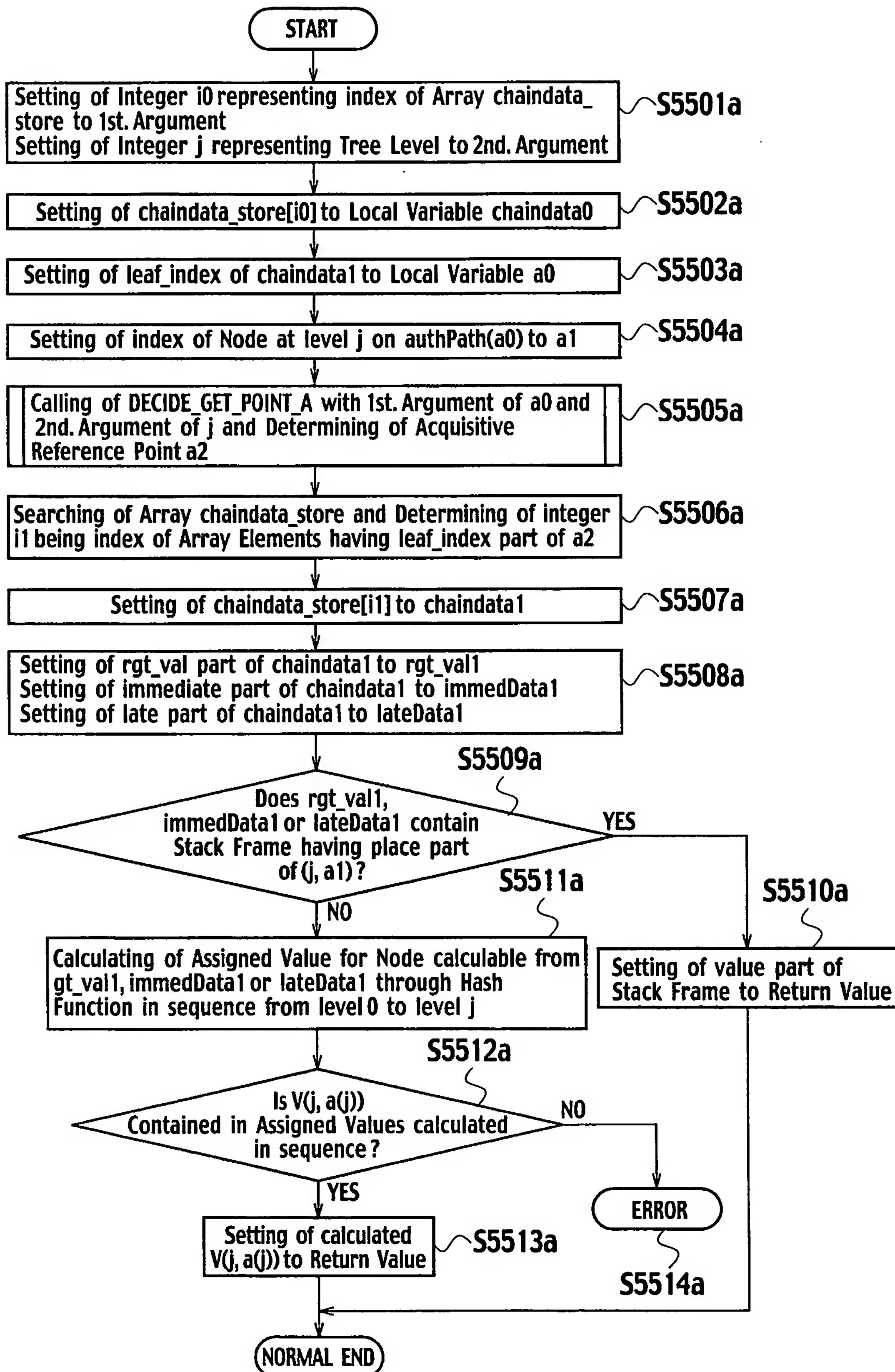
FIG. 41



49 / 77
FIG. 55

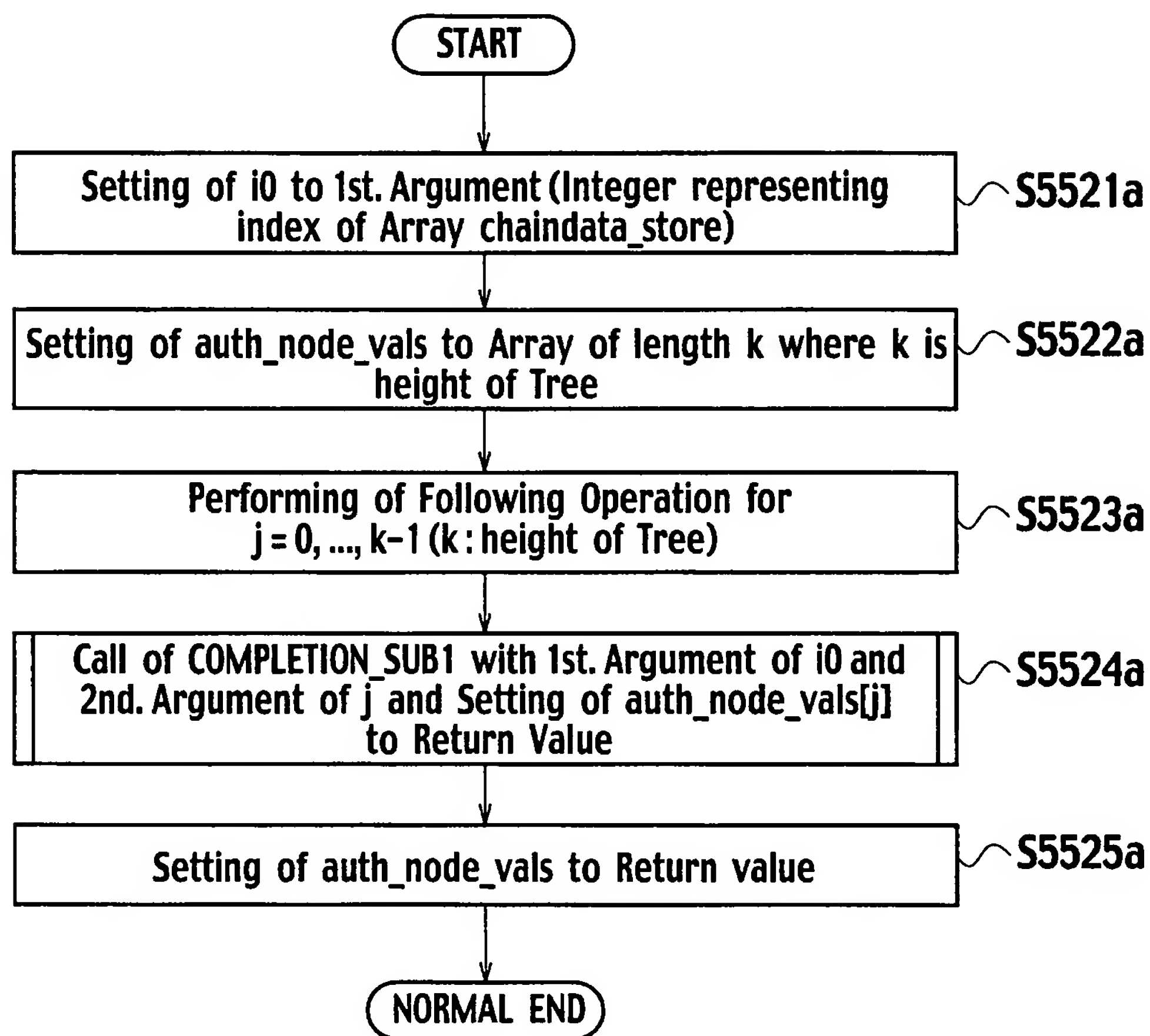


60 / 77
FIG. 66

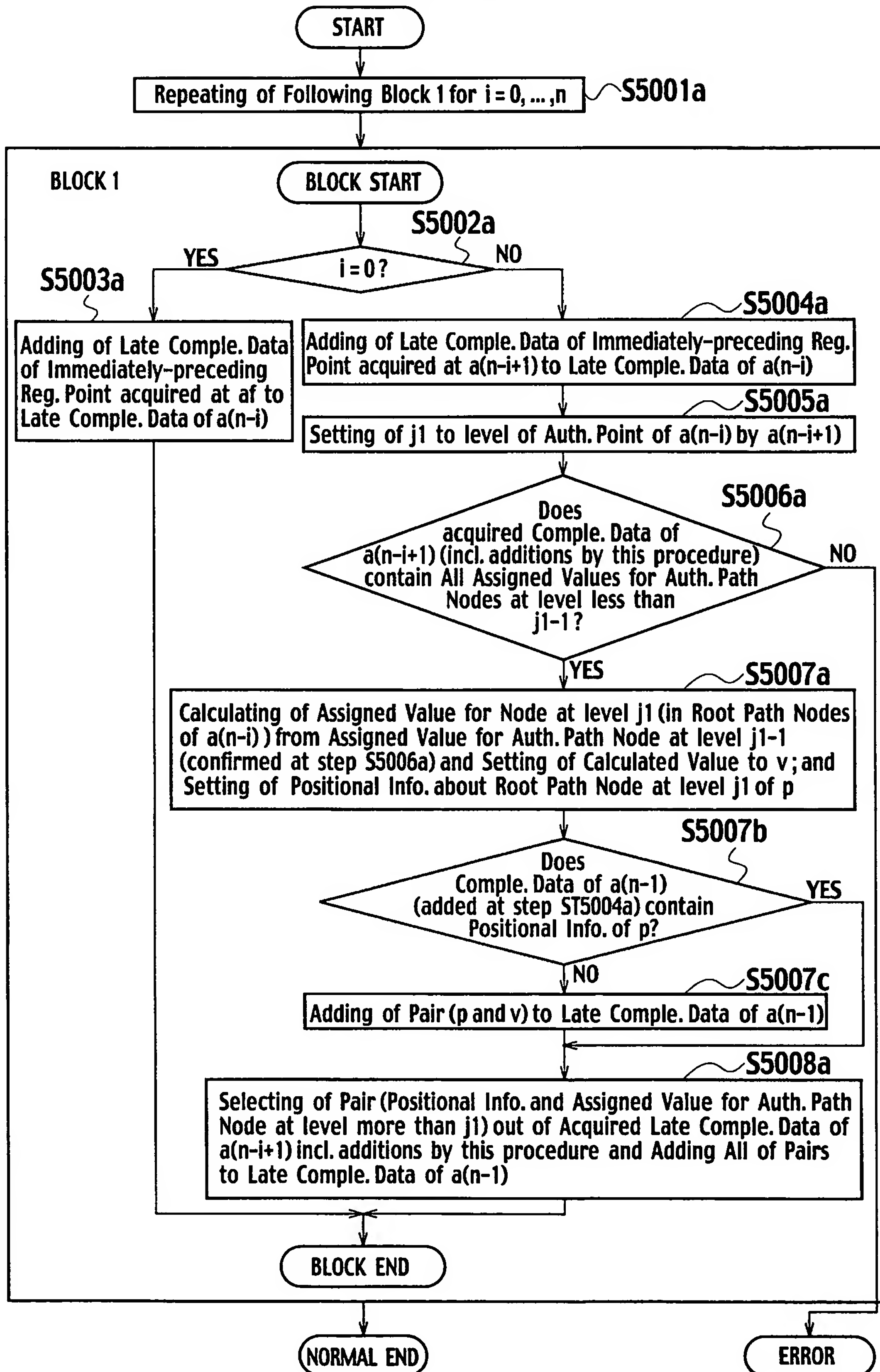


61 / 77

FIG. 67



62 / 77
FIG. 68



70 / 77

FIG. 76

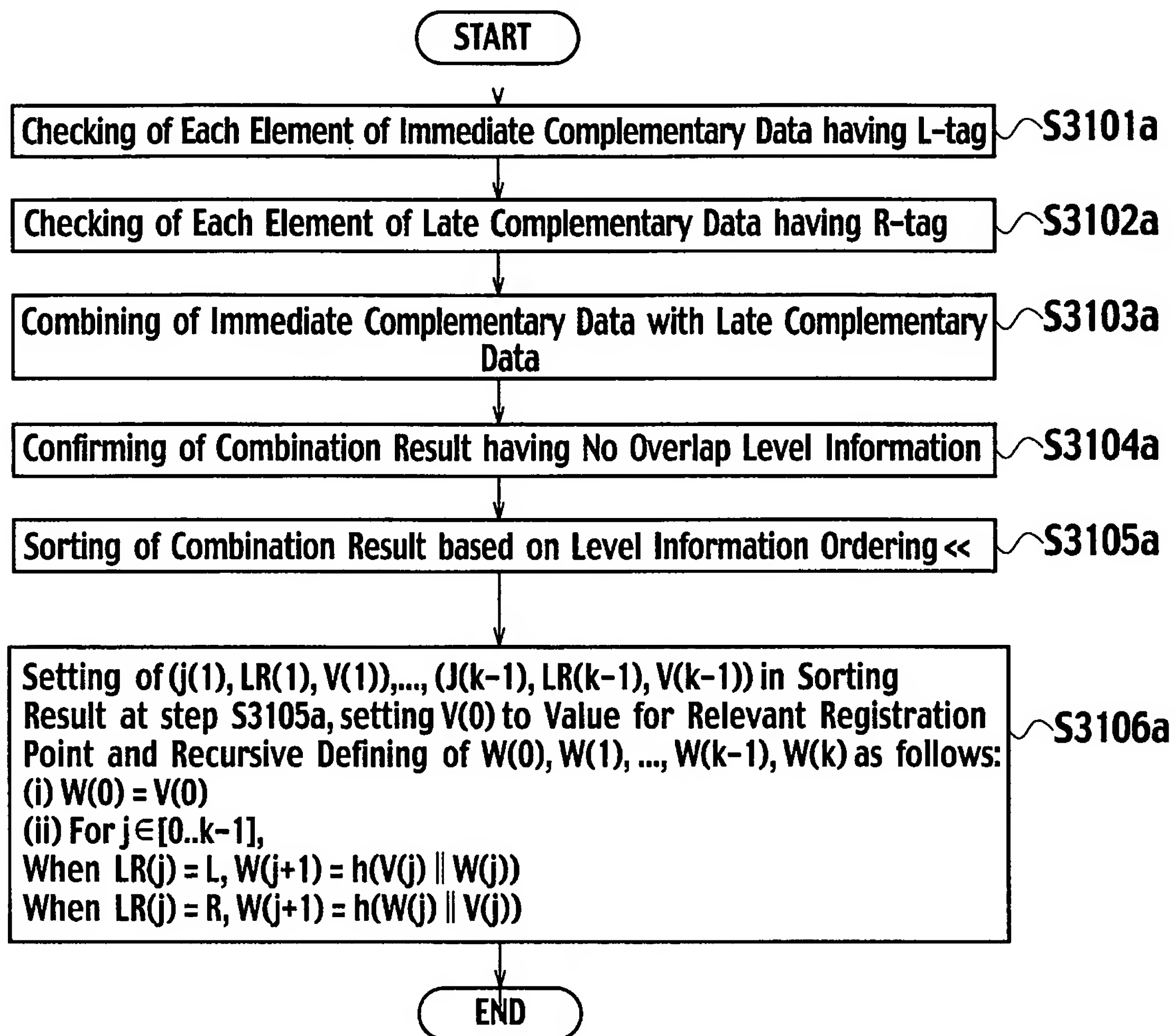


FIG. 77

